UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	CRIMINAL NO. 21-cr-10104-PBS
VLADISLAV KLYUSHIN Defendant	)	

MOTION TO ACQUIT FOR IMPROPER VENUE

Now comes the defendant Vladislav Klyushin, by and through undersigned counsel, and hereby moves for judgment of acquittal, under Fed. R. Crim. P. 29(c),[1] on the ground that the evidence presented at trial, viewed most favorably to the government, fails to establish venue in this district as a matter of law.

Venue issues are

> animated in part by the danger of allowing the government to choose its forum free from any external constraints. The ever-increasing ubiquity of the Internet only amplifies this concern. As we progress technologically, we must remain mindful that cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue. People and companies still exist in identifiable places in the physical world. When people commit crimes, we have the ability and obligation to ensure that they do not stand to account for those crimes in forums in which they performed no essential conduct element of the crimes charged.[2]

[1] This motion is filed without prejudice to Mr. Klyushin's other dismissal and acquittal arguments made before and during trial, which are expressly reserved for any appeal he may pursue.

[2] *U.S. v. Auernheimer*, 748 F.3d 525, 541 (CA3 2014) (all citations, alterations and internal punctuation omitted unless otherwise noted).

Venue is generally "determined from the nature of the crime alleged and the location of the act or acts constituting it."[3] To make that determination, courts must "[1] initially identify the conduct constituting the offense … and then [2] discern the location of the commission of the criminal acts."[4] And in applying prong one, the court must take care to "separate 'essential conduct elements' from 'circumstance elements.'"[5] "Only 'essential conduct elements' can provide the basis for venue; 'circumstance elements'" – simply "facts that existed at the time … the defendant performed" the criminal "acts" constituting the offense – "cannot."[6]

As the Court instructed the jury, the essential conduct elements of the crimes charged in this case "involved" Klyushin or a co-schemer "misrepresenting" their "identity online to access computer systems to obtain material nonpublic information to trade on the confidential information."[7] None of those essential conduct elements – accessing protected computers and obtaining confidential information by misrepresenting identity – took place in the District of Massachusetts. To be sure, they inescapably occurred in at least the districts where Toppan

[3] *U.S. v. Anderson*, 328 U.S. 699, 703 (1946); *accord U.S. v. Rodriguez-Moreno*, 526 U.S. 275, 279 (1999); *U.S. v. Cabrales*, 524 U.S. 1, 6-7 (1998).

[4] *Rodriguez-Moreno*, 526 U.S. at 279.

[5] *Auernheimer*, 748 F.3d at 533 (quoting *Rodriguez-Moreno*, 526 U.S. at 280 & n.4) (*Auernheimer* alterations omitted).

[6] *Auernheimer*, 748 F.3d at 533 (citing *U.S. v. Bowens*, 224 F.3d 302, 310 (CA4 2000)); *see also id.* at 534 n.4 (distinguishing "essential *conduct* element[s]" from essential *offense* elements to be proved beyond a reasonable doubt, and stressing that the former are narrower than the latter) (emphasis supplied).

[7] T. 10-129-30 (Feb. 10, 2023).

Merrill's and DFIN's "servers" were "located" and duplicitously "accessed."[8] But in stark contrast, "[n]o protected computer was accessed and no data … obtained"[9] here in Boston.

At most, the record shows that Boston was a mere "pass through"[10] – a site that allegedly happened to be associated with an intermediate IP address assigned at random by a Virtual Private Network (VPN).[11] And, tellingly, the government offered no evidence that Klyushin or his reputed cohorts purposely availed themselves of a Boston-based IP address or consciously actuated its use – much less that the latter was within their knowledge or even reasonably foreseeable. Far from an essential conduct element, then, any remote and attenuated connection to Massachusetts or this district was an incidental fortuity – the epitome of a "circumstance element."[12] It follows that the verdict cannot stand.

The government's own manual for prosecuting computer crime illustrates the point. As discussed there at length:

> Multidistrict offenses "may be . . . prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Note that only the "essential conduct elements" of a crime qualify. *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280 (1999). For instance, section 1030(a)(2)(C) prohibits intentionally accessing a computer without or in excess of authorization, and thereby obtaining information from any protected computer. The two essential conduct elements in section 1030(a)(2)(C) are

[8] *Auernheimer*, 748 F.3d at 533-34.

[9] *Ibid.* 534.

[10] Computer Crime & Intellectual Prop. Section, US DOJ, *Prosecuting Computer Crimes 119*, *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual. pdf (last visited Mar. 10, 2023) (DOJ Manual).

[11] The Boston IP address was just one of 100+ IP addresses used to access the servers of Toppan and DFIN – and so used, at that, only from late Oct.-early Nov. 2018. There is no evidence that any of the other IP addresses mentioned at trial had any connection to the District of Massachusetts.

[12] *Rodriguez-Moreno*, 526 U.S. at 280 n.4.

"accessing" a computer and "obtaining" information. Thus, it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access *and* where the information is obtained.

The exact location of each event—the "accessing" and the "obtaining"— may not always be easily determined.

> Example: *An intruder located in California uses communications that pass through a router in Arizona to break into a network in Illinois and then uses those network connections to obtain information from a server in Kentucky.*

The intruder initiated access in California, and **the router in Arizona enabled that access**. Arguably, however, the intruder did not achieve access until reaching the network in Illinois. Of course, one could also argue that access did not occur until the intruder reached the server in Kentucky where the information was located. Likewise, one could argue that the intruder obtained the information in Kentucky, or that he did not obtain the information until it reached him in the district where he was located, in this case, California.

This example illustrates an offense governed by 18 U.S.C. § 3237(a). Under any of the options discussed above, **the appropriate venue would seem to include both of the endpoints—that is, the district in which the offender is located (California) and the district in which the information is located (Kentucky)**. It is likely that venue is also proper at some, if not all, of the points in between, since venue may lie "in any district in which [a continuing] offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Under this section, the "accessing" and "obtaining" arguably continued in Arizona and Illinois. **Certainly, venue seems proper in Illinois where the intruder broke into the network. *Whether the intruder committed a crime in Arizona is less clear***.

Prosecutors looking to fix venue in the locale through which communications passed, as in the case of the router in Arizona, should look closely at the facts to determine whether venue in that district would satisfy the framework discussed above. **The case for "pass through" venue may be stronger where transmission of the communications themselves constitutes the criminal offense** (e.g., when a threatening email is sent in violation of 18 U.S.C. § 1030(a)(7)) **and the path of transmission is certain** …. By contrast, ***in cases where the path of transmission is unpredictable, a court may find it difficult to conclude that a crime was committed in a district merely because packets of information***

> ***happened to travel through that district***…. Of course, where the "pass through" computer itself is attacked, venue would likely be proper based on the attack, without reference to pass-through rationale.
>
> Federal prosecutors should also take note of the Department of Justice's policies for wire and mail fraud, which may be analogous. For wire fraud, section 967 of the Department's Criminal Resource Manual provides that prosecutions "may be instituted in any district in which an interstate or foreign transmission was **issued or terminated**." Crim. Resource Manual § 967. Although the text of section 967 refers only to the place of issuance or termination, the case cited in support of that proposition, *United States v. Goldberg*, 830 F.2d 459, 465 (3d Cir. 1987), relies on 18 U.S.C. § 3237(a), which also includes the place where the conduct continued, thus leaving open the door to "pass through" venue. In the case of mail fraud, section 9-43.300 of the U.S. Attorneys' Manual states that **Department of Justice policy "opposes mail fraud venue based solely on the mail matter passing through a jurisdiction**." USAM 9-43.300; *see also* Crim. Resource Manual § 966.[13]

This case's Massachusetts IP address substantially mirrors the "pass through" Arizona router that enabled access in the DOJ Manual. And a close – even cursory – "look" at our facts indicates neither that "transmission of the communications themselves constitutes the criminal offense" nor that "the path of transmission [wa]s certain." Rather, since the path of transmission was "unpredictable" – passing through Boston purely by chance – it is "difficult to conclude that a crime was committed in [this] district merely because packets of information happened to travel through th[is] district." Forcing Klyushin to defend here thus implicated squarely the "extraordinarily important" and "deep … public policy" concerns – around the "unfairness and hardship" of "haul[ing]" an accused to trial in a "distant, remote, or unfriendly forum solely at the

[13] DOJ Manual 118-20 (all emphasis supplied except in "Example").

prosecutor's whim" – that led the framers to enshrine "two" separate venue "safeguard[s]" in the Constitution.[14]

The government cannot shake these concerns – or disavow the conclusion dictated by its own manual and *Auernheimer* – by seeking to salvage Count One through the expedient of 18 USC § 3238, the so-called "high seas" venue provision. **First**, no essential *conduct* underlying the charged hack-and-trade conspiracy[15] – *i.e.*, *misrepresenting identity online* to access protected computers and thereby obtain confidential information for trading purposes[16] – occurred outside the United States.[17] Instead, the critical deception alleged – impersonating Toppan and DFIN employees by fraudulently misusing their credentials to log in to the companies' computers and steal their data – was exclusively domestic, confined strictly to the districts housing those computers.

Second, and relatedly, "Art. III, § 2, cl. 3 of the Constitution provides that all criminal trials, except in cases of impeachment, 'shall be held in the State where the said Crimes shall have been committed; but *when not committed within any State*, the Trial shall be at such Place or Places as the Congress may by Law have directed.'"[18] In turn, § 3238 – titled "Offenses not committed in any district" – represents an exercise of Congress's constitutionally reserved "power [to] direct[] by law the place of trial of crimes 'not committed within any State,'" intended to apply only "where

---

[14] *Aurenheimer*, 748 F.3d at 540-41.

[15] *See* Dkt. 197.

[16] T. 10-129-30.

[17] *See*, *e.g.*, *U.S. v. Miller*, 808 F.3d 607, 609-10 (CA2 2015) (recognizing that "essential offense conduct test" governs application of § 3238 as well as § 3237); *U.S. v. Mallory*, 337 F. Supp. 3d 621 (E.D. Va. 2018) (same), *aff'd*, 40 F.4th 166 (CA4 2022), *cert. pet. filed* (Dec. 1, 2022).

[18] *Chandler v. U.S.*, 171 F.2d 921, 931 (CA1 1948) (emphasis supplied) (footnote omitted).

'there is no court which has particular cognizance of the crime.'"[19] Belatedly deploying a "cryptic" and "opaque" statute[20] – one properly "focus[ed]" on foreign "offense conduct"[21] – to backfill venue for a crime that plainly *was* committed in the American states and districts housing Toppan's and DFIN's computers smacks of forum shopping. Worse, it inverts the rule of lenity and defies the absolute and emphatic command of Art. III, § 2, cl. 3, rendering § 3238 unconstitutional as applied in this case.[22] In effect, a contrary holding would allow the government to prosecute in any district it chooses any foreign national whose conduct significantly touches, substantially impacts and largely takes place within identifiable districts in the United States. That is not, and cannot be, the law.

For all these reasons, the Court should overturn the jury's verdict, enter a judgment of acquittal and dismiss the indictment.

---

[19] *Ibid.*; *accord*, *e.g.*, *U.S. v. Rodriguez*, 182 F. Supp. 479, 494 (S.D. Cal. 1960) (§ 3238 specifies trial venue for "alleged criminal acts … committed in foreign countries"); *aff'd in part, rev'd in part on other grounds*, 288 F.2d 545 (CA9 1961); *U.S. v. Wan Lee*, 44 F. 707, 709 (D. Wash. No. Div. 1890) (materially identical predecessor statute "gives the rule by which to locate the jurisdiction in criminal cases where the offenses are committed outside of any district").

[20] *Miller*, 808 F.3d 619.

[21] *Ibid.*

[22] *See* Dkt. 193.

Respectfully Submitted,

Vladislav Klyushin,
By His Attorney,

/s/ Maksim Nemtsev
Maksim Nemtsev, Esq.
Mass. Bar No. 690826
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700
menemtsev@gmail.com

/s/ Marc Fernich
Marc Fernich
Law Office of Marc Fernich
800 Third Avenue
Floor 20
New York, NY 10022
212-446-2346
Email: maf@fernichlaw.com

Dated: March 13, 2023

CERTIFICATE OF SERVICE

I, Maksim Nemtsev, hereby certify that on this date, March 13, 2023, a copy of the foregoing documents has been served via Electronic Court Filing system on all registered participants.

/s/ Maksim Nemtsev
Maksim Nemtsev, Esq.